REMARKS

In the Office Action, the Examiner rejected claims 1-20. No claims are presently added, amended, or canceled. Applicants respectfully request reconsideration of the claims in view of the remarks set forth below.

Rejections Under 35 U.S.C. § 103

In the Office Action, the Examiner rejected claims 1-12 and 14-19 under 35 U.S.C. § 103(a) as being unpatentable over Quinn et al., U.S. Patent No. 5,720,293 (hereinafter "Quinn") in view of Osborn, U.S. Patent No. 6,026,293 (hereinafter "Osborn"); rejected claim 13 under 35 U.S.C. § 103(a) as being unpatentable over Quinn and Osborn as applied to claim 9; and rejected claim 20 under 35 U.S.C. § 103(a) as being unpatentable over Quinn and Osborn as applied to claim 19, and further of view of Ali et al., U.S. Patent No. 6,584,336 (hereinafter "Ali"). Applicants respectfully traverse these rejections.

Legal Precedent

The burden of establishing a *prima facie* case of obviousness falls on the Examiner. *Ex parte Wolters and Kuypers*, 214 U.S.P.Q. 735 (B.P.A.I. 1979). To establish a *prima facie* case, the Examiner must not only show that the combination includes *all* of the claimed elements, but also a convincing line of reason as to why one of ordinary skill in the art would have found the claimed invention to have been obvious in light of the teachings of the references. *Ex parte Clapp*, 227 U.S.P.Q. 972 (B.P.A.I. 1985). In establishing a *prima facie* case for obviousness, "the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background the obviousness or nonobviousness of the subject matter is determined." *KSR Int'l Co. v. Teleflex, Inc.*, 127 S. Ct. 1727 at 1729 (2007).

It is improper to combine references where the references teach away from their combination. *In re Grasselli*, 713 F.2d 731, 743, 218 U.S.P.Q. 769, 779 (Fed. Cir. 1983); M.P.E.P. § 2145. Moreover, if the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *In re Ratti*, 270 F.2d 810, 123 U.S.P.Q. 349 (C.C.P.A. 1959); *see* M.P.E.P. § 2143.01(VI). If the proposed modification or combination would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *In re Gordon*, 733 F.2d 900, 221 U.S.P.Q. 1125 (Fed. Cir. 1984); *see* M.P.E.P. § 2143.01(V).

The Examiner rejected claims 1-12 and 14-19 under 35 U.S.C. § 103(a) as being unpatentable over the Quinn reference in view of the Osborn reference. Specifically, the Examiner stated:

> Claims 1 - 12, and 14 - 19 are rejected ' under 35 U.S.C. 103(a) as being unpatentable over Quinn et al. (USPN. 5,720,293 - previously cited) in view of Osborn (USPN 6,026,293 - previously cited). Quinn et al. teach a medical device that may include a pulse oximeter (column 4, lines 8 - 13; column 5, lines 16 - 20) that includes a digital memory configured to provide a security function for identifying the device and preventing tampering with memory related to the medical device (column 5, lines 41 - 64; column 10, line 61 - column 13, line 31). Quinn et al. teach an exemplary implementation of the security encoding that includes use of encrypting/decrypting keys (column 11, line 65 - column 12, line 35) and further teach that alternate known encoding schemes can be used. Further, Quinn et at. teach that the monitoring system includes elements to read and verify the security information and that the memory may be included in a connector portion (considered to be "an adapter coupled between the sensor and the monitor") (column 5, lines 41 - 64; Figure 1 and column 4, lines 33 - 46). Quinn et al. 'teach that encoding portions of the data stored in the sensor memory provides added protection of the data (column 11, line 66 -,column 12, line 55). Thus, Quinn et al. teach all of the features of the claimed invention except they do not particularly teach that this is

> implemented with a digital signature. Osborn teach an arrangement for preventing electronic memory tampering that is useful in medical instrument operation (column 1, lines 9 - 16) that includes use of digital signatures to protect sensitive data from unauthorized access. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Quinn et al. to use a digital signature, as taught by Osborn, since Quinn et al. indicate that their device may be implemented with alternate digital security features and Osborn teach that use of a digital signature in a medical device provides these security features.
>
> Office Action, pp. 2 and 3.

Applicants respectfully traverse this rejection. The Quinn reference states that it is desirable for information in a memory to be coded to prevent unauthorized access. Quinn, col. 3, lines 48-49. More specifically, the Quinn reference states that the purpose of encoding the data in the memory is to make if more difficult to copy or counterfeit the catheters made by a particular manufacturer. Quinn, col. 11, line 66 – col. 12, line 3. "For this purpose an algorithm is used to encode selected bites of data within the catheter EPROM." Quinn, col. 12, lines 3-4. The Quinn reference then lists a number of important data items that are stored in encoded form in order to prevent copying and counterfeiting. *See*, Quinn, col. 4, line 12 – col. 13, line 31. The Quinn reference also describes a specific algorithm that is preferable to use to encode and decode the stored data. Quinn, col. 12, lines 17-36.

To generally summarize the disclosure of the Quinn reference, it appears that certain data must be stored in memory in an encoded form in order to prevent copying or counterfeiting. If the catheter with the encoded data in its memory is connected to an appropriate monitor, a proprietary algorithm on the monitor is capable of decoding the encoded data so that the catheter can only be effectively used with an approved monitor.

Generally the Osborn reference, on the other hand, does not disclose that encoded data is stored in memory. Rather, it states that the contents of memory may be periodically hashed so that the hash value may be compared to a valid hash value previously derived from the authentic

memory contents. Osborn, col. 6, lines 31-39. The Osborn reference further describes that a public/private key authentication scheme may be used to authenticate a device prior to allowing the device to access stored data. Col. 6, line 46 – col. 7, line 3. In one example, following the authentication of a requesting device and its reprogramming of its memory contents, a new hash value may be calculated based on the modified memory contents, and the new has value is returned to the data transfer device for a digital signature. Osborn, col. 7, lines 4-12. Hence, the Osborn document may generally disclose that data is stored in a memory in unencoded form, and that the stored data is used to create a digital signature through the use of a hashing operation and encryption via private key.

Based on the disclosures of the Quinn and Osborn references, it is clear that the Quinn reference cannot be modified by the Osborn reference to obtain the claimed subject matter as alleged by the Examiner. Since the memory disclosed in the Quinn reference stores encoded or encrypted data, which can only be decrypted by an authorized monitor, there would be no need to provide further authentication by the attachment of a digital signature to the encrypted data. Indeed, if any modification of the Quinn reference were to take place in view of the teachings of the Osborn reference, it would be to store data in the catheter memory of the Quinn reference in unencoded form and to use the data to form a digital signature which could be exchanged with the monitor to authenticate its right to access the unencoded data. However, such as modification would be antithetical to the clearly stated purpose of the Quinn reference, which is to prevent copying or counterfeiting of memory contents. Indeed, many methods exist for determining the contents of a memory, such as using a logic analyzer to intercept the transfer of the memory contents while the catheter is connected to an authorized device, and thereafter, using the intercepted contents to create counterfeit devices. Consequently, there is no reasonable modification of the Quinn device that would lead to storage of a digital signature on the catheter memory.

This position is bolstered by the well-known use of the two techniques described in the Quinn and Osborn references. For example, Applicants have attached a document entitled

"What is a digital signature?" as Exhibit 1. As can be seen on page 1 of Exhibit 1, data may be encrypted prior to transmission and decrypted upon receipt in order to protect unauthorized access to the actual data. This technique is very similar to the technique described in the Quinn reference. As an alternative, on pages 2 and 3 of Exhibit 1, a digital signature may be used to authenticate the transmission and receipt of raw data. Specifically, the stored raw data may be hashed to create a message digest, and the message digest may be encrypted with a private key to create a digital signature. *Id.*, p. 2. The digital signature is then attached to the raw data and sent to another user. *Id.* Upon receipt of the signed raw data, the raw data is hashed to create a message digest, and the digital signature is decrypted with a public key to recreate the original message digest used to create the digital signature. If the data has been transferred in an uncorrupted form, the hash value (message digest) of the transferred data should match the hash value (message digest) of the original authentic data. If authentic, the raw data may then be used for various purposes such as updating memory content, or facilitating further data transfers. This alternative method of transfer appears to be very similar to the method disclosed in the Osborn reference.

It should be noted that these data transfer methodologies and authentication processes are disclosed in the alternative. In other words, it would be superfluous to attach a digital signature to a message comprising encrypted data downloaded from a memory. Accordingly, this unbiased extrinsic evidence relating to the use of these data transfer techniques confirms Applicants' position that the Quinn and Osborn references could not be combined in a manner to render the claimed subject matter obvious. Consequently, Applicants respectfully request withdrawal of the Examiner's rejection and allowance of all pending claims.

Applicants also explicitly traverse the Examiner's rejection of claim 20 because one of the references relied upon by the Examiner is not believed to be prior art. The Examiner rejected claim 20 under 35 U.S.C. § 103(a) as being unpatentable over Quinn and Osborn in view of Ali. However, the earliest priority claimed by Ali is October 26, 1999, which disqualifies Ali as prior art. According to the Declaration Under 37 C.F.R. § 1.131, which was filed in the present case

on March 17, 2006, the subject matter of the present application was conceived prior to June 9, 1999, and diligently pursued until the filing date of the present application. Accordingly, Ali is not prior art with respect to the present application. In view of the Examiner's mistaken reliance on a reference (i.e., Ali) that is not prior art, Applicants respectfully request that, if the Examiner deems a future official action necessary, that it be made non-final.

Conclusion

In view of the remarks and amendments set forth above, Applicants respectfully request allowance of the pending claims. If the Examiner believes that a telephonic interview will help speed this application toward issuance, the Examiner is invited to contact the undersigned at the telephone number listed below.

Payment of Fees and General Authorization for Extensions of Time

A three month extension fee of $1,050 is believed to be due. In accordance with 37 C.F.R. § 1.136, Applicants hereby provide a general authorization to treat this and any future reply requiring an extension of time as incorporating a request for such an extension. The Commissioner is authorized to charge the requisite fee of $1,050 for a three month extension and any additional fees which may be required to the credit card listed on the attached PTO-2038. However, if the PTO-2038 is missing, if the amount listed thereon is insufficient, or if the amount is unable to be charged to the credit card for any other reason, the Commissioner is authorized to charge Deposit Account No. 06-1315; Order No. TYHC:0053-2 (P0230S-02).

Respectfully submitted,

Date: 3/11/08

Michael G. Fletcher
Reg. No. 32,777
FLETCHER YODER
P.O. Box 692289
Houston, TX 77269-2289
(281) 970-4545

What is a Digital Signature?

An introduction to Digital Signatures, by David Youd

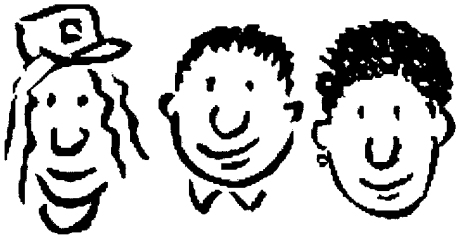
Bob

(Bob's public key)

(Bob's private key)

Bob has been given two keys. One of Bob's keys is called a Public Key, the other is called a Private Key.

Bob's Co-workers:



Pat Doug Susan

Anyone can get Bob's Public Key, but Bob keeps his Private Key to himself

Bob's Public key is available to anyone who needs it, but he keeps his Private Key to himself. Keys are used to encrypt information. Encrypting information means "scrambling it up", so that only a person with the appropriate key can make it readable again. Either one of Bob's two keys can encrypt data, and the other key can decrypt that data.

Susan (shown below) can encrypt a message using Bob's Public Key. Bob uses his Private Key to decrypt the message. Any of Bob's coworkers might have access to the message Susan encrypted, but without Bob's Private Key, the data is worthless.

"Hey Bob, how about lunch at Taco Bell. I hear they have free refills!"

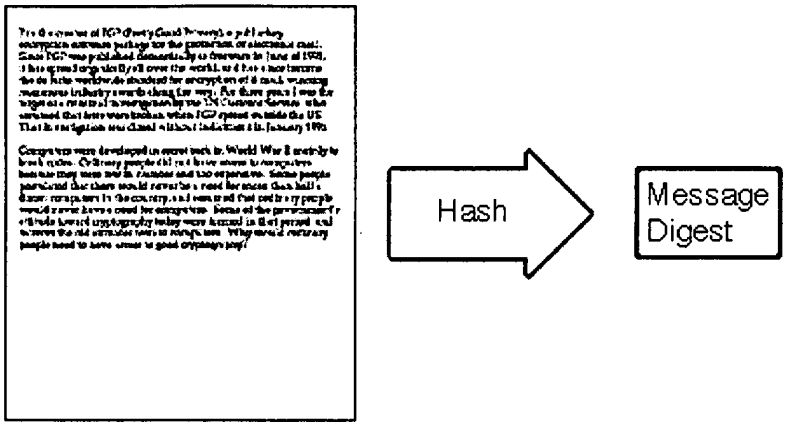
HNFmsEm6Un
BejhhyCGKOK
JUxhiygSBCEiC
0QYIh/Hn3xgiK
BcyLK1UcYiY
lxx2lCFHDC/A

HNFmsEm6Un
BejhhyCGKOK
JUxhiygSBCEiC
0QYIh/Hn3xgiK
BcyLK1UcYiY

"Hey Bob, how about lunch at Taco Bell. I hear they have free refills!"

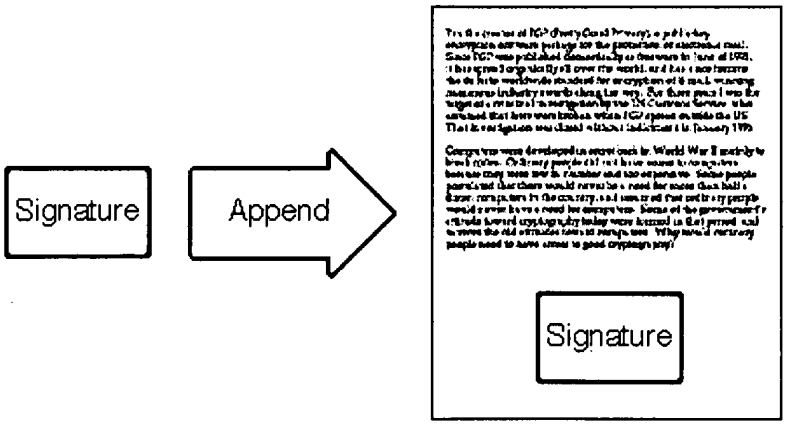
lxx2lCFHDC/A

With his private key and the right software, Bob can put digital signatures on documents and other data. A digital signature is a "stamp" Bob places on the data which is unique to Bob, and is very difficult to forge. In addition, the signature assures that any changes made to the data that has been signed can not go undetected.

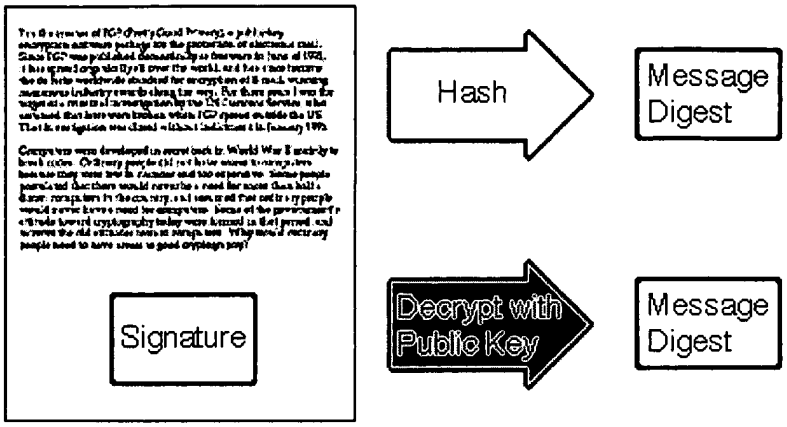


To sign a document, Bob's software will crunch down the data into just a few lines by a process called "hashing". These few lines are called a message digest. (It is not possible to change a message digest back into the original data from which it was created.)

Bob's software then encrypts the message digest with his private key. The result is the digital signature.



Finally, Bob's software appends the digital signature to document. All of the data that was hashed has been signed.



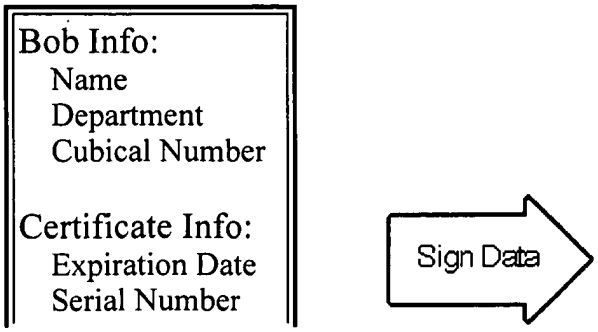
Bob now passes the document on to Pat.

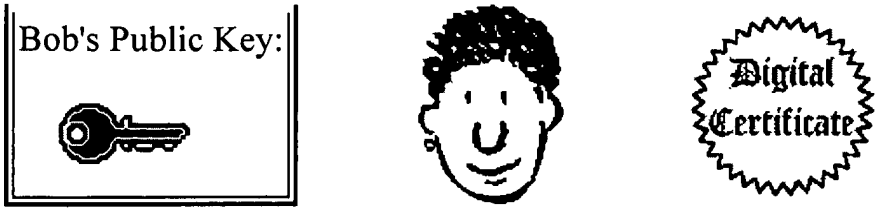
First, Pat's software decrypts the signature (using Bob's public key) changing it back into a message digest. If this worked, then it proves that Bob signed the document, because only Bob has his private key. Pat's software then hashes the document data into a message digest. If the message digest is the same as the message digest created when the signature was decrypted, then Pat knows that the signed data has not been changed.

Plot complication...

Doug (our disgruntled employee) wishes to deceive Pat. Doug makes sure that Pat receives a signed message and a public key that appears to belong to Bob. Unbeknownst to Pat, Doug deceitfully sent a key pair he created using Bob's name. Short of receiving Bob's public key from him in person, how can Pat be sure that Bob's public key is authentic?

It just so happens that Susan works at the company's certificate authority center. Susan can create a digital certificate for Bob simply by signing Bob's public key as well as some information about Bob.

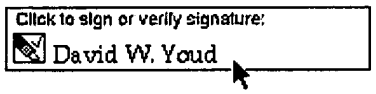




Now Bob's co-workers can check Bob's trusted certificate to make sure that his public key truly belongs to him. In fact, no one at Bob's company accepts a signature for which there does not exist a certificate generated by Susan. This gives Susan the power to revoke signatures if private keys are compromised, or no longer needed. There are even more widely accepted certificate authorities that certify Susan.

Let's say that Bob sends a signed document to Pat. To verify the signature on the document, Pat's software first uses Susan's (the certificate authority's) public key to check the signature on Bob's certificate. Successful de-encryption of the certificate proves that Susan created it. After the certificate is de-encrypted, Pat's software can check if Bob is in good standing with the certificate authority and that all of the certificate information concerning Bob's identity has not been altered.

Pat's software then takes Bob's public key from the certificate and uses it to check Bob's signature. If Bob's public key de-encrypts the signature successfully, then Pat is assured that the signature was created using Bob's private key, for Susan has certified the matching public key. And of course, if the signature is valid, then we know that Doug didn't try to change the signed content.



Although these steps may sound complicated, they are all handled behind the scenes by Pat's user-friendly software. To verify a signature, Pat need only click on it.

Warning: You may be missing a few lines of text if you print this document. This seems to occur on pages following pages that have blank space near the bottom due to moving tables with large graphics in them to the next page so that the images are not split across pages. If this happens to you, simply print out document in sections. (Ex: I have the problem on page 4, so I print pages 1-3, then pages 4-5.)

Click to go back to
THE YOUD ZONE